REMARKS

The Examiner has objected to the claims. Such objection is deemed avoided by virtue of the clarifications made hereinabove to the claims.

The Examiner has rejected Claims 19 and 20 under 35 U.S.C. 101 because the claimed invention is non-statutory. Such rejection is deemed avoided in view of the clarifications made hereinabove to the claims.

The Examiner has rejected Claims 1-19 under 35 U.S.C. 102(e) as being anticipated by Vaidya (U.S. Patent No. 6,279,113). Applicant respectfully disagrees with such rejection, especially in view of the amendments made hereinabove to each of the independent claims. Specifically, applicant has amended each of the independent claims to at least substantially include the subject matter of former dependent Claims 11-12 et al.

The Examiner has relied on the following excerpts (as well as the figures) from Vaidya to make a prior art showing of applicant's claimed "data monitoring device ... configured to monitor network traffic, decode protocols" (see this or similar, but not necessarily identical language in each of the independent claims).

> "Although the data collectors 10 are illustrated as stand-alone devices, the function of a data collector can be included on other devices in the network, such as a server or a router/firewall/switch 20. Multiple data collectors 10 are preferred when the LAN 11 includes multiple network objects which the IDS must monitor for network intrusions. As will be discussed in greater detail below, allocating monitoring responsibilities among multiple data collectors 10 in such situations tends to maintain a high performance of the IDS. Two of the data collectors 10 are deployed on first and second LAN segments 14 and 16 each of which includes multiple workstations, a third data collector 10 is located on a server backbone 18 of the LAN 11 to monitor network traffic to and from the servers, a fourth data collector 10 is located proximate to the router/firewall/switch 20 to monitor incoming data to the LAN 11, and a fifth data collector monitors incoming data to a remote network 24." (Col. 5, lines 9-25)
>
> "The virtual processor 36 obtains a data packet from a queue and extracts MAC header information, IP header information, transport

> header information, and application information from the data packet. Extraction of the packet information enables the data collector 10 to detect network intrusions based in the different layers of the OSI model." (Col. 7, lines 17-24)

The Examiner continues by arguing that applicant's claimed data monitoring device is met by item 10 of Figure 1 from Vaidya. The Examiner then continues by relying on the following excerpt from Vaidya to make a prior art showing of applicant's claimed "application program interfaces configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection" (see this or similar, but not necessarily identical language in each of the independent claims).

> "Each data collector 10 includes a communication module 34 for transmitting and receiving information to and from the data repository 12. A configuration builder module 32 assigns a set of signature profiles to each network object and stores data representative of associations between network objects and attack signature profile sets in a signature profile memory 39. The configuration builder module 32 accesses the appropriate attack signature profile sets during operation of the data collector 10 and provides the attack signature profiles to a stateful dynamic signature inspection (SDSI) virtual processor 36." (Col. 6, lines 1-11)

The Examiner continues by arguing the following:

> "Application program interface is defined as 'a set of functions or methods used to access some functionality'. Referring to Fig. 2, the configuration builder module (item 32) allows the intrusion detection device (item 36) access attack signature profiles stored in signature profile memory (item 39), as described in column 6 lines 1 to 11. Also, the communication module (item 34) allows intrusion detection device access the data in database handler (item 26). This clearly allows the intrusion detection device access the functionality of the data-monitoring device to perform intrusion detection, and hence discloses the feature. Therefore, the Examiner asserts that Vaidya discloses the feature by inheritance."

It thus appears that the Examiner is relying on item 32 and 34 to meet applicant's claimed application program interfaces. However, it also appears that the Examiner is relying on item 10 (which includes item 36) to meet both applicant's claimed intrusion

detection device and data monitoring device. Applicant respectfully disagrees with this assertion, as item 10 only includes one processor, namely 36), and therefore can not meet applicant's claimed "application program interfaces configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection," as claimed. It is clear that Vaidya only suggests one processor, an intrusion detection module only, without a separate data monitoring device, and therefore does not require the application program interfaces claimed by applicant.

The Examiner is reminded that a claim is anticipated only if each and every element as set forth in the claim is found, either expressly or inherently described in a single prior art reference. *Verdegaal Bros. v. Union Oil Co. Of California*, 814 F.2d 628, 631, 2 USPQ2d 1051, 1053 (Fed. Cir. 1987). Moreover, the identical invention must be shown in as complete detail as contained in the claim. *Richardson v. Suzuki Motor Co.*868 F.2d 1226, 1236, 9USPQ2d 1913, 1920 (Fed. Cir. 1989). The elements must be arranged as required by the claim.

This criterion has simply not been met by the above reference, as noted above. Nevertheless, despite such paramount deficiencies and in the spirit of expediting the prosecution of the present application, applicant has amended each of the independent claims to further distinguish applicant's claim language from the above reference, as follows.

> "a data monitoring device comprising a capture engine operable to capture data passing through the network in response to a trigger and configured to monitor network traffic, decode protocols for grouping packets into different protocol presentations and assembling the packets into high level protocol groups, and analyze received data for managing the network by collecting statistics, and detecting broken lines, traffic loads, and network errors;
>
> an intrusion detection device separate from the data monitoring device, the intrusion detection device comprising a detection engine operable to perform intrusion detection on data provided by the data monitoring device;

application program interfaces configured to allow the intrusion detection device access to applications of the data monitoring device to perform intrusion detection; and

memory for storing reference network information used by the intrusion detection device to determine if an intrusion has occurred;

wherein the application program interfaces allow the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device" (emphasis added).

In particular, applicant has amended the independent claims to include the subject matter of Claims 11-12 et al. With respect to the subject matter of former Claims 11-12 et al. (now at least substantially incorporated into each of the independent claims), the Examiner has relied on the foregoing excerpts from Vaidya to make a prior art showing of applicant's claimed technique "wherein the application program interfaces allow the intrusion detection device to leverage the separate data monitoring device, by allowing the intrusion detection device to call an application program interface configured to open a protocol decoding application associated with the separate data monitoring device, and by allowing the intrusion detection device to call an application program interface configured to open an alarm generation application associated with the separate data monitoring device" (see this or similar, but not necessarily identical language in each of the independent claims). It is clear, however, as noted above, that Vaidya does not meet applicant's claimed separate data monitoring device, let alone the claimed application program interfaces. For similar reasons, the present claimed specific application program interfaces are also not met.

Still yet, to further distinguish the prior art of record, applicant has amended each of the independent claims to emphasize the specific functionality of the data monitoring

device, the manner in which the different application program interfaces are called, the separate nature of the data monitoring device, etc.

A notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Still yet, applicant brings to the Examiner's attention the subject matter of new Claims 21-22 below, which are added for full consideration:

"wherein at least one of the application program interfaces take the form of frame_context_pointer_position" (see Claim 21); and

"wherein at least one of the application program interfaces include:

frame_tcp_bridge,

frame_udp_bridge,

frame_ip_bridge, and

frame_http_bridge" (see Claim 22).

Again, a notice of allowance or specific prior art showing of each of the foregoing claim elements, in combination with the remaining claimed features, is respectfully requested.

Thus, all of the independent claims are deemed allowable. Moreover, the remaining dependent claims are further deemed allowable, in view of their dependence on such independent claims.

In the event a telephone conversation would expedite the prosecution of this application, the Examiner may reach the undersigned at (408) 505-5100. The

Commissioner is authorized to charge any additional fees or credit any overpayment to Deposit Account No. 50-1351 (Order No. NAI1P317/01.185.01).

Respectfully submitted,
Zilka-Kotab, PC.

Kevin J. Zilka
Registration No. 41,429

P.O. Box 721120
San Jose, CA 95172-1120
408-505-5100